NOT FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

MANDAR MIRASHI,

Plaintiff,

v.

JOHN DOE,

Defendant (unknown individual)

v.

521.99931468 Bitcoin,

In rem Defendant

v.

FIXED FLOAT, KRAKEN, CHANGENOW, EXCH.CX, TRADEOGRE, & JOHN DOE EXCHANGE(S)

Relief Defendants

No. 25cv1805 (EP) (LDW)

OPINION

Plaintiff Mandar Mirashi alleges that an unknown perpetrator (the "Hacker") hacked his email and cryptocurrency wallets and stole approximately $40 million worth of Bitcoin from his cryptocurrency wallets. D.E. 1 ("Complaint" or "Compl."). Plaintiff moves for an *ex parte* temporary restraining order ("TRO") generally freezing Plaintiff's stolen Bitcoin. D.E. 2-1. ("TRO Motion" or "TRO Mot."). Plaintiff also moves *ex parte* for expedited discovery to obtain information pertaining to the identity of the Hacker and to determine the current location of Plaintiff's stolen Bitcoin. D.E. 3-1 ("Discovery Motion" or "Discovery Mot.") (together with the TRO Motion, the "Motions").

The Court has reviewed the Motions and all other relevant items on the docket and decides the Motions without oral argument. *See* Fed. R. Civ. P. 78(b); L. Civ. R. 78.1(b). For the following reasons the Court will **GRANT** both Motions and will order regular status updates to the Court.

I. BACKGROUND

As of February 27, 2025, Plaintiff owned 521.99931468 Bitcoin which he kept in two cryptocurrency wallets with blockchain addresses 36cfw3QiQeJJryX7JbWb1DKL7ZP1zMuF1S ("Plaintiff Wallet 1") and 33oV5phadHeUPEgjVNH9fVUZsNhAeDLhAN ("Plaintiff Wallet 2"). D.E. 2-2 ("Pl. Decl.") ¶ 3.

On the afternoon of February 25, 202[5], Plaintiff received an email purporting to be from Google concerning account access by relatives of a deceased person. *Id.* ¶¶ 4-5. Plaintiff clicked on a link titled "Case File," entered his Google login credentials on the page that link opened, and was directed to what appeared to be a Google chat portal where he attempted to inquire into the account access notification. *Id.* ¶¶ 6-7.

Later that evening, Plaintiff received an email from "support+recover@ledger.com," which appeared to be from Ledger, a brand of "cold storage" wallet used to keep cryptocurrency keys secure. *Id.* ¶¶ 9-10. The email referred to a "recovery request" that Plaintiff had submitted, and stated that if Plaintiff had not submitted a recovery request, he needed to take immediate action by clicking on a link in the email, providing his "extended public key" and requesting that the recovery request be cancelled. *Id.* ¶ 12. Plaintiff had not initiated a recovery request and contacted Ledger to inform them that he believed he was the target of a phishing scam. *Id.* ¶¶ 13-14. Plaintiff exchanged emails with Ledger but is unaware which emails were legitimate and which emails were not. *Id.* ¶ 15.

Plaintiff turned to Reddit for guidance and posted on a Reddit page asking if others had seen similar emails from Ledger. *Id.* ¶ 19. After receiving various conflicting reports from the Reddit community, Plaintiff noticed that his Reddit account had been deleted by an unknown user and he could no longer access the responses to his post. *Id.* ¶¶ 20-22.

The night of February 26, 2025, in light of the suspicious activity, Plaintiff moved 300 BTC out of his Ledger wallet and into another cryptocurrency wallet, Electrum, and went about changing various passwords, including his Google password. *Id.* ¶¶ 24-25. Plaintiff never clicked on the link contained in the February 25 email from support+recover@ledger.com and never provided his "extended public key" or "private key" details to anyone. *Id.* ¶ 26.

However, that same night, Plaintiff saw a pending transaction on the Bitcoin blockchain which attempted to move 302 BTC from Plaintiff's Electrum wallet to an address he was not familiar with: bc1q8fvx5trkyfvt9xmj43pmum9de76lhq0euntngr. *Id.* ¶ 27. Plaintiff immediately took steps to halt this transaction and was successful in preventing it from moving forward. *Id.* ¶ 28. Believing that his Electrum wallet was compromised, Plaintiff moved his Bitcoin back to his Ledger wallet. *Id.* ¶ 29.

The next day, February 27, 2025, Plaintiff discovered that 521.99931468 BTC had been transferred from his two Ledger wallets and sent to the following address: bc1q8fvx5trkyfvt9xmj43pmum9de76lhq0euntngr. *Id.* ¶ 30. Smaller amounts of other cryptocurrency assets were also missing from Plaintiff's Ledger and Metamask wallets and the wallets were left completely empty. *Id.* ¶ 31. Plaintiff subsequently contacted the police and the FBI. *Id.* ¶ 32.

To assist in tracking and recovering the missing Bitcoin, Plaintiff retained Blockchain Forensic Roman Bieda ("Blockchain Forensic"), a Blockchain analysis company. TRO Mot. at 2.

On March 5, 2025, Blockchain Forensic submitted a report on the "theft and subsequent movements" of Plaintiff's Bitcoin. *Id.* (citing D.E. 2-4 ("BF Report")). Blockchain Forensic concluded the following:

- The Hacker transferred 521.99931468 BTC from Plaintiff's wallets to the Hacker's address: bc1q8fvx5trkyfvt9xmj43pmum9de76lhq0euntngr. BF Report ¶ 12.
- The funds were then "distributed through a complex layering system designed to conceal the source of the money." *Id.* From the Hacker's address the Bitcoin was split up and spread out in 668 transactions to 197 different "singe-use" private (unhosted) addresses and to 140 addresses associated with blockchain services. *Id.* ¶¶ 12-14.
- Approximately 354.4 of Plaintiff's Bitcoin was deposited in accounts held by the following cryptocurrency companies: FixedFloat, Kraken, ChangeNow, exch.cx, TradeOgre, and unknown (John Doe) Exchange(s) (together, the "Relief Defendants"). *Id.* ¶ 14.
- Another approximately 139.41 BTC remain in wallets controlled by the Hacker:
    - bc1qedyy7dfqz7kcesk8ap5kv0sq90c0cctv75fjda;
    - bc1q5uhs4kwaq685hx2p9klhzufw6kzck65x9znvua;
    - bc1qwjtuqew73j8zhc0xhezx905fvytj5g4307czjf;
    - 35sBUp4t5t8gerEu9HswPiNhRSTnnS8qWX; and
    - 38WP9sta67jMzwPrzWfrGMci7qVCpX4cFY. *Id.* ¶ 16.
- 29.19 BTC was spent on blockchain transaction fees or dissipated, and the destination is still unknown. *Id.* ¶ 17.

On March 12, 2025, Plaintiff filed the Complaint, TRO Motion, and Discovery Motion. Plaintiff alleges that the Hacker is liable under the following causes of action: Computer Fraud and Abuse Act[1] ("CFAA") (Count I), New Jersey Computer-Related Offenses Act[2] (Count II), Fraud (Count III), Conversion (Count IV), Replevin under N.J.S.A. 2B:50-1 (Count V), and Unjust Enrichment (Count VI). Compl ¶¶ 77-110. Plaintiff also seeks equitable relief against the Hacker and the Relief Defendants enjoining current and future holders of the stolen assets from transferring or disposing and disgorging such assets and seeks a constructive trust over the assets and an accounting of the assets (Count VII). *Id.* ¶¶ 111-119. Plaintiff also seeks compensatory, consequential, and punitive damages, interest, fees, and costs. *Id.* at 18-19.

II. LEGAL STANDARDS

A. TRO Motion

Federal Rule of Civil Procedure 65(b) governs the issuance of TROs without notice to the adverse party. A court may issue a TRO under such circumstances only if

> (A) specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition; and
>
> (B) the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required.

Fed. R. Civ. P. 65(b)(1). Furthermore, every TRO issued without notice "must state the date and hour it was issued; describe the injury and state why it is irreparable; state why the order was issued without notice; and be promptly filed in the clerk's office and entered in the record." Fed. R. Civ. P. 65(b)(2). The court must set the TRO to expire within 14 days "unless before that time the

[1] 18 U.S.C. §1030 *et seq*.
[2] N.J.S.A. § 2A:38A.

court, for good cause, extends it for a like period or the adverse party consents to a longer extension." *Id.*

To obtain a preliminary injunction or a TRO, the plaintiff must make a threshold showing: (1) a likelihood of success on the merits of his claim, and (2) the plaintiff will be irreparably harmed if the injunction is not granted. *Reilly v. City of Harrisburg*, 858 F.3d 173, 176 (3d Cir. 2017). Additionally, when relevant, courts should take into account "the possibility of harm to other interested persons from the grant or denial of the injunction," and "the public interest." *Id.* (cleaned up).

B. Discovery Motion

Federal Rule of Civil Procedure 26(d)(1) generally prohibits discovery "before the parties have conferred as required by Rule 26(f)." However, district courts have broad discretion over their own dockets and how discovery proceeds. *See In re Fine Paper Antitrust Litig.*, 685 F.2d 810, 817 (3d Cir. 1982). Rule 26(d) does not specify when expedited discovery should be permitted. In the absence of guidance from the Rules, courts in this District generally rely on the "good cause standard." *Strike 3 Holdings, LLC v. Doe*, No. 18-2674, 2020 WL 3567282, at *4 (D.N.J. June 30, 2020) (collecting cases).

"Under the good cause test, whether to permit expedited discovery is decided by considering the totality of the circumstances and the balancing of the interests of the plaintiff and defendant." *Id.* Factors courts consider generally include:

> (1) the timing of the request in light of the formal start to discovery; (2) whether the request is narrowly tailored; (3) the purpose of the requested discovery; (4) whether the discovery burdens the defendant; and (5) whether the defendant can respond to the request in an expedited manner

Id.

III. ANALYSIS

A. The Court Will Grant the TRO Motion

1. Likelihood of success on the merits

As a general rule, courts may not freeze a defendant's assets as part of a TRO or preliminary injunction in a case where only money damages are sought. *Grupo Mexicano de Desarrollo S.A. v. Alliance Bond Fund, Inc.*, 527 U.S. 308, 333 (1999). However, Plaintiff seeks the equitable remedy of a constructive trust over the stolen Bitcoin assets. "There is an exception to the general ban on prejudgment asset restraints where an equitable remedy is sought." *Nail All., LLC v. TTN Beauty*, No. 21-3140, 2021 WL 2646989, at *2 (D.N.J. Mar. 10, 2021). Therefore, as the TRO seeks such asset restraints, the Court will focus on Plaintiff's conversion, unjust enrichment, and constructive trust claims, which provide for the availability of the equitable relief Plaintiff seeks.

The "elements of conversion are: (1) 'the property and right to immediate possession thereof belong to the plaintiff' and (2) 'the wrongful act of interference with that right by the defendant.'" *Latef v. Cicenia*, No. A-5747-13T2, 2015 WL 10458543, at *5 (N.J. Super. Ct. App. Div. Mar. 14, 2016) (quoting *First Nat'l Bank v. N.J. Trust Co.*, 18 N.J. Misc. 449, 452 (N.J. 1940)).[3]

The elements of unjust enrichment are: (1) the "defendant received a benefit"; (2) the "retention of that benefit without payment would be unjust"; (3) the plaintiff "expected remuneration"; and (4) the "failure to give remuneration unjustly enriched the defendant."

[3] Plaintiff resides in New Jersey and alleges that a significant portion of the acts that give rise to his claims occurred through his computer in New Jersey. Compl. Therefore, under the "most significant relationship" test as required by New Jersey's choice-of-law jurisprudence, the Court applies New Jersey law. *See Portillo v. Nat'l Freight, Inc.*, 323 F. Supp. 3d 646, 651 (D.N.J. 2018).

EnviroFinance Grp., LLC v. Env't Barrier Co., 113 A.3d 775, 790 (N.J. Super. Ct. App. Div. 2015).

The elements of a claim for constructive trust under New Jersey law are (1) a "wrongful act"; (2) "caused the property to come into the hands of the recipient"; and (3) "the recipient will be 'unjustly enriched' if it is not returned." *Thompson v. City of Atlantic City*, 901 A.3d 428, 438 (N.J. Super. Ct. App. Div. June 28, 2006).

Based on the events set forth in Plaintiff's affidavit and the BF Report and discussed above, the Court finds that Plaintiff has demonstrated a likelihood of success on the merits of his conversion, unjust enrichment, and constructive trust claims.

2. Irreparable harm

In cases involving theft of cryptocurrency, many courts have recognized that the failure to promptly freeze the cryptocurrency leads to irreparable harm. *See, e.g.*, *Song v. Doe*, No. 24-809, 2024 WL 4632242, at *3 (M.D. Fla. Aug. 19, 2024) ("Plaintiff will suffer irreparable injury if the TRO is not granted because Defendants can quickly transfer the assets to another untraceable cryptocurrency wallet or to offshore entities organized in unknown locations."); *Yogaratnam v. Dubois*, No. 24-393, 2024 WL 758387, at 4 (E.D. La. Feb. 23, 2024) ("Plaintiff has shown that irreparable harm will ensue absent a TRO, considering the speed with which cryptocurrency transactions are made, as well as the anonymous nature of those transactions."); *Heissenberg v. Doe*, No. 21-80716, 2021 WL 8154531, at *2 (S.D. Fl. Apr. 23, 2021) ("Because of the speed and potential anonymity of cryptocurrency transactions, the Plaintiff is likely to suffer immediate and irreparable injury if a temporary restraining order is not granted."). The same is true here.

3. Harm to others and the public interest

As alleged, the assets at issue rightfully belong to Plaintiff and nobody else. According to the Complaint, Plaintiff's affidavit, and the BF Report, Plaintiff's Bitcoin was stolen from his

cryptocurrency wallets and is in the process of being "distributed through a complex layering system designed to conceal the source of the money." BF Report ¶ 12. Therefore, it is not apparent that there is any significant harm to others or to the public interest that would result if the TRO is granted.

4. Notice is not required

Plaintiff's attorney has certified that neither he nor Plaintiff knows the identify of the Hacker. D.E. 2-3 ("Gonnelli Decl.") ¶ 5. Plaintiff's attorney also states that alerting the Hacker that Plaintiff is seeking to require the Relief Defendants and recipients of the stolen Bitcoin to freeze the assets would likely prompt the Hacker to take more "extreme measures" to "conceal and dissipate the stolen Bitcoin." *Id.* The Court agrees and finds that notice is not required here.

Therefore, for the foregoing reasons, the Court will **GRANT** Plaintiff's TRO Motion and enter a TRO freezing Plaintiff's stolen Bitcoin that will expire within 14 days subject to further extension by consent or good cause shown.

B. The Court Will Grant the Discovery Motion

Plaintiff seeks expedited discovery to accomplish two goals: identify the Hacker and locate his stolen Bitcoin. Discovery Mot. at 4. To achieve those goals, Plaintiff seeks discovery from the Relief Defendants and the following third-parties: Google LLC, Ledger SAS, Onfido, Electrum, Verizon Communications, Inc., and Reddit, Inc. (collectively the "Third Parties").

The Relief Defendants are virtual asset service providers ("VASPs") that Plaintiff, informed by the BF Report, believe received his stolen Bitcoin. Discovery Mot. at 4. Without discovery from the Relief Defendants, Plaintiff avers that he cannot track his stolen Bitcoin because the transactions of the depositor which follow the deposit into the VASPs are not public. *Id.* Furthermore, Plaintiff believes the Relief Defendants collect information regarding the

depositors, including the depositor of Plaintiff's stolen Bitcoin. Plaintiff seeks discovery of this information. Discovery Mot. at 4-6.

As alleged, the Third Parties likely have relevant information about the theft. Plaintiff believes that the Hacker hacked Plaintiff's Google account to access information that enabled the Hacker to respond to Plaintiff with false emails and to assume Plaintiff's identity. Pl. Decl. ¶¶ 4-8. The Ledger phishing email sent February 25, 2025 stated that Plaintiff's drivers' license would be sent to Onfido. *Id.*, Ex. C. Plaintiff alleges the Hacker stole Bitcoin directly from his Ledger wallets and attempted to steal Bitcoin from his Electrum wallet. *Id.* ¶¶ 27, 30. Plaintiff believes that the Hacker used Reddit to advise him to comply with the February 25, 2025 email from support+recover@ledger.com seeking information about Plaintiff's credentials and was responsible for his account deletion. *Id.* ¶¶ 20, 22; Discovery Mot. at 8. Therefore, Plaintiff believes Reddit may have information on the identify of the Hacker and the devices, IP addresses, and ISPs used by the Hacker. Plaintiff also asserts that, as his internet service provider ("ISP"), Verizon keeps relevant information about traffic on their networks and it is likely Verizon has records of the Hacker's access to Plaintiff's computer such as the IP address and machine identifiers of the devices used to access Plaintiff's computer. Discovery Mot. at 8. Plaintiff seeks records from the Third Parties that are associated with the Hacker's access to the services.

Considering the factors described in *Strike 3 Holdings, LLC*, the Court finds that good cause exists to order the requested discovery on an expedited basis.

IV. CONCLUSION

For the foregoing reasons, the Court will **GRANT** both the TRO Motion and the Discovery Motion. The Court will construe the TRO Motion as also seeking a preliminary injunction and order expedited briefing and set a hearing on the motion. Appropriate Orders follow.

Dated: March 12, 2025

Evelyn Padin, U.S.D.J.